International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 November 2023*

Database Security Issues and Challenges in Cloud Computing

Dr. Karuturi S R V Satish
Data Services Engineer, Software Engineering
JP Morgan Chase & Co
New Jersey, USA
karutoori@gmail.com

Abstract—The majority of enterprises have recently enthusiastically embraced cloud computing, and at the same time, the database has moved to the cloud. This cloud database paradigm can lower data administration expenses and free up new business to concentrate on the product that is being delivered. Furthermore, issues with scalability, flexibility, performance, availability, and affordability can be resolved with cloud computing. Security, however, has been noted as posing a serious risk to cloud databases and has been essential in fostering public acceptance of cloud computing. Several security factors should be taken into account before implementing any cloud database management system. These features comprise, but are not restricted to, data privacy, data isolation, data availability, data integrity, confidentiality, and defense against insider threats. In this paper, we discuss the most recent research that took into account the security risks and problems associated with adopting cloud databases. In order to better comprehend these problems and how they affect cloud databases, we also provide a conceptual model. Additionally, we look into these problems to the extent that they are relevant and provide two instances of vendors and security features that were used for cloud-based databases. Finally, we provide an overview of the security risks associated with open cloud databases and suggest possible future paths.

Keywords-Cloud Computing, Database Security, Cloud Database Management System, Data Security

I. INTRODUCTION

When applications are supplied as services over the Internet, along with the hardware and system software that are housed in the data centers that offer those services, this is referred to as cloud computing [1]. The public, private, and hybrid clouds are the three fundamental deployment models of the cloud computing paradigm [2]. Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are the three primary types of cloud computing services [2]. Furthermore, a novel form known as database-as-a-service (DBaaS) has been discovered lately; according to its standards, it may belong to any of these primary categories [3].

The acceptance of cloud computing has been largely influenced by security concerns. Executing your software on someone else's hard drive while utilizing someone else's CPU can be frightening to many, much as the concept of placing your important data there. Data loss, phishing, and botnets are examples of security problems that pose serious risks to an organization's software and data [2]. In addition, the cloud computing model's multi-tenancy structure and shared computing resources have created new security risks (like Botcloud Attack), which call for innovative solutions [2].

DBaaS, often known as cloud database, is a unique type of database intended for use in virtualized computer environments, or cloud environments. Its primary purpose is the cloud storage of large amounts of data [4]. Database as a Service (DBaaS) is emerging as a viable method of offering reliable and adaptable data storage services to cloud applications, given the diverse uses of cloud applications[5]. The scalability, performance, availability, and cost issues are resolved by cloud-based IT systems [6]. Cloud databases require more than just setting up a relational database on a cloud server; they also require optimizing the database's performance and adding extra nodes online as needed. Microsoft SQL Azure, Amazon RDS, and Apache Cassandra database are a few prominent DBaaS examples [7]. Relational or NoSQL databases can be used as the general type of database in cloud computing. Not Only SQL, or NoSQL, databases are helpful for large-scale semi-structured and unstructured data processing applications, including big data [8]. The four primary models used by NoSQL databases to store data are document-based, graph-based, key-value, and column-oriented [8]. NoSQL databases are an excellent option for cloud computing infrastructure since they are typically built to scale across several data centers and operate as distributed systems [9].

However, maintaining several dispersed copies of the database at different places is quite difficult. In order to access and manage cloud data, a secure framework must be used to access and manage the cloud database [10]. Adoption of cloud databases may encounter difficulties with (1) effective multi-tenancy, (2) elastic scalability, and (3) database security and privacy [7]. Moreover, organizations have determined that database security is the primary problem in this industry due to the trade-off between data security and scalability and cost savings [6]. A database belonging to Adobe Creative Cloud recently revealed 7.5 million client records, which were then made public online.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 November 2023*

Adobe Systems Inc. verified that a vulnerability resulting from an improperly setup prototype environment was the cause of the data leakage. Email addresses, product subscriptions, payment statuses, login updates, and other information were among the exposed data. These details might potentially be exploited in social engineering attacks, resulting in account takeover and identity theft, among other things [11]. Additionally, the Cloud Security Alliance (CSA), a preeminent group that establishes best practices to guarantee a safe cloud computing environment. According to significance, the company reported the following top cloud computing security threats in 2019 [12]: insider threats, insecure interfaces and APIs, weak control plane, failures of the megastructure and infrastructure, limited visibility and abuse of cloud services, data breaches, misconfiguration and inadequate change control, lack of cloud security architecture and strategy, insufficient identity, credential, access and key management, account hijacking, and insider threats.

In this paper, we discuss the difficulties and security concerns associated with adopting a cloud database. The remainder of the document is organized as follows. Some comparable works and surveys in the same topic of study are included in Section 2. The architecture of cloud databases is reviewed in Section 3. The security concerns with cloud databases are covered in Section 4. Discussion and analysis are presented in Section 5, and a summary of the unresolved problems that need more research is given in Section 6. This paper is concluded in Section 7.

II. RELATED WORK

The relevant research in the field of cloud databases can be divided into surveys that covered broad topics and surveys that went into greater detail into specific security topics like auditing [13] and encryption [14] in cloud computing. The variations and parallels between these research, which include our study, are displayed in Table 1. Deka et al.'s assessment [18] covered fifteen well-known cloud databases, giving a summary of each system's storage platform, licensing type, and programming language. Cassandra is an open-source Java system that stores data as a column-oriented database; it is an example of a NoSQL database. Another illustration is ClearDB, an open-source database built in C/C++ on the MySQL platform [8].

The history of NoSQL databases was given by Han et al. [15], whose writers began by drawing comparisons between NoSQL and conventional databases. They then described the features and data model of a NoSQL database, as well as its benefits and drawbacks. The three data models—Key-value, Column-oriented, and Document—are classified according to the consistency, availability, and partition tolerance CAP theorem and are each explicitly specified by database examples. Lastly, the writers suggest that before choosing to employ a NoSQL database, businesses should review a list of alternatives that includes the following: data model, CAP Support, multi-data center support, capacity, performance, query API, dependability, data persistence, rebalancing, and business support.

Researchers in [16] looked on the insider danger in cloud relational databases and how the layout of the cloud database can impact security flaws by making it easier for insiders to initiate attacks. The three mitigating models in the proposed solution—the Peer-to-Peer, Centralized, and Mobile Knowledgebases models—were developed based on the impact of insiders' knowledge bases and controlled query execution following insider knowledge base checks (profiling insider activities). In order to prevent an attack from being launched by a combination of data items that an insider could obtain from available data zones, load balancing was also suggested as a control mechanism for the previously suggested models.

Researchers gave a thorough analysis of cloud computing security in [18]. This work addressed the security risks and challenges associated with each cloud model and service type. Next, it covered the general threats associated with cloud computing, which include a variety of vulnerabilities like data breaches, denial of service (DoS) attacks, vulnerabilities in API browsers, malicious insider attacks, and more. The writers then went on to outline the defenses against the dangers that had been previously mentioned. Countermeasures include business continuity plans, secure Interfaces and APIs, end-to-end encryption, screening for malicious activity (such as firewalls and intrusion detection systems, or IDS), and cloud consumer validation.

A paper that attempts to categorize cloud SaaS security patterns was developed by authors in [27]. The authors of this work were inspired to provide a fresh source of official security best practices and security knowledge documentation for cloud SaaS application developers to utilize as a reference. They divided cloud SaaS security patterns into five areas. The first is compliance and regulatory, which has to do with rules controlling how data is processed and used in the cloud. The authorization, authentication, and identification make up the second pattern. The secure development, operation, and administration pattern is the third one. The fourth pattern was all about secrecy and seclusion. A secure architecture is the final pattern. The most well-known cloud SaaS providers, AWS and Azure, have security solutions that were compared by the authors as they wrapped up their investigation. Table 1 contrasts the current surveys and displays the suggested survey's position in this study with regard to how previous surveys addressed security concerns and cloud database environment solutions.

TABLE 1. Related Surveys

Study Reference	Include Security solutions	Include Security threats& attacks	Study field		Include real examples of Cloud providers			
			Cloud Computing	Cloud DB	AWS	Azure	Oracle	Google
[8]	-	-	-	√	-	-	-	-
[15]	-	-	-	√	-	-	-	-
[16]	√	√	-	√	-	-	-	-
[13]	√	√	√	√		-	-	-
[14]	√	-	√	√		-	-	-
[17]	√	√	√	-	-	-	-	-
[18]	√	√	√	-	√	√		

III. CLOUD DATABASE STRUCTURE

Cloud computing database environments come in several flavors. For example, some employ a multi-instance

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 November 2023*

architecture, while others use a multi-tenant approach. With the multi-instance feature, every user has access to a separate database management system (DBMS) that runs on a virtual machine (VM), giving them total control over a variety of security-related duties. While the multi-tenant model gives cloud users access to a predetermined environment that they can share with other tenants—usually by assigning each tenant's data a unique user ID. In the latter case, maintaining a secure database environment is the responsibility of the cloud service provider [19].

A cloud database management system's five-layered design was presented by the authors in [20], as seen in Fig 1. The first of the five levels is the external layer, which interacts with users. It is followed by the conceptual middleware layer, which conceals the specifics of heterogeneity in the conceptual layer, which uses several database types, including DB2, SQL, and Oracle. The conceptual layer takes care of data processing and replaces the database's overall logical structure. The physical middleware layer conceals the specifics of the several heterogeneous platforms that are used, including Windows, macOS, and Linux. The physical layer, which is the final layer, is concerned with how data is physically represented.

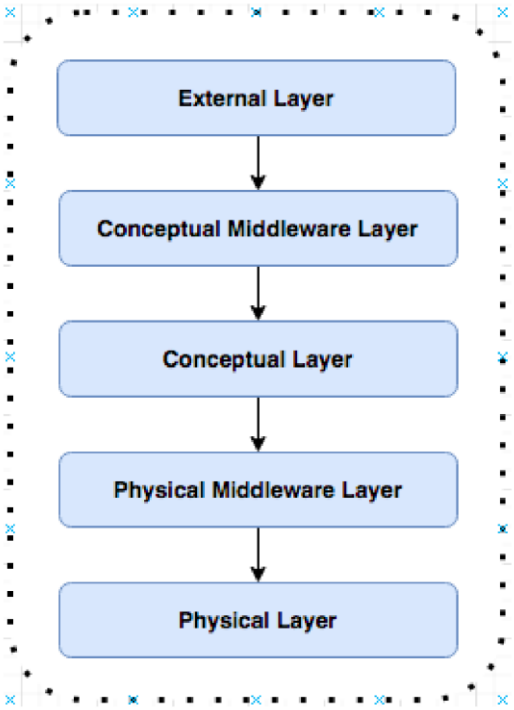

Figure 1. Cloud Database Management System [20]

A cloud database allows for the sharing and distribution of data among multiple places, with the added benefit of authentic information and specific privileges. As a result, ensuring data security, scalability, and consistency is crucial. A DBMS for cloud data is required to handle these and other data-related concerns. In general, shared-nothing and shared disk are the two primary DBMS designs utilized in cloud environments [27]. First off, a shared-nothing distributed computing architecture is one in which every node is independent of every other node and can function independently, meaning that each node has its own memory and disk storage without having to share them. Second, a computational design known as shared disk architecture combines memory on each node with shared disk storage.

As each database server processes and stores a portion of the database, it divides the data. Since shared disk and shared nothing systems have drawbacks and problems, a lot of work has been done in the field of cloud database management system architecture [10,20].

IV. Cloud Database Security and Data Protection Challenges

The idea that DBaaS is a fantastic choice for businesses with less funding has been discussed [14]. But it can also result in a lot of security problems because a third party (i.e., the provider) takes over the maintenance of the database and its underlying security instead of the data owner. One of the main risks to the data kept in cloud storage is security [14]. As a result, we examine the most recent security concerns in cloud databases in this part, working our way up from data-level security issues to general security concerns in the cloud database ecosystem.

Large amounts of data are distributed and shared among numerous tenants in cloud computing; for this reason, data protection is essential when storing data in cloud databases [10]. The four main obstacles to data protection are privacy, isolation, availability, integrity, and confidentiality of data [19, 21].

A. Data Confidentiality

When storing private or confidential data in a cloud database, users must take data confidentiality seriously. Data confidentiality is ensured through the use of authentication and access control mechanisms. By boosting cloud resilience, problems with access control, authentication, and data secrecy in cloud computing can be resolved. Moreover, cryptography can ensure data secrecy; however, this cannot be achieved with basic encryption since it will cause issues with key management and be unable to accommodate sophisticated database needs like query, parallel modification, and fine-grained authorization. It is hard to maintain confidentiality by carelessly encrypting the private data within a cloud database, as classical encryption impedes the execution of SQL queries through a DBMS engine. For instance, querying encrypted data might be an extremely slow computing procedure.

- *Homomorphic Encryption*

Generally, encryption is intended to protect the privacy of data; Rivest proposed homomorphic encryption. Data operations in the cloud and data confidentiality can be

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 November 2023*

resolved by implementing this encryption. It guarantees that the results obtained from the ciphertext match those obtained from the clear text; additionally, the process does not necessitate the decryption of the data. A significant advancement in this kind of encryption is that the completely homomorphic encryption approach can accomplish any action that can be carried out in plain text without the need for decryption. On the other hand, the encryption process performs the extremely complex calculation, requiring a large amount of processing power and storage. Ultimately, practical uses for completely homomorphic encryption are still a ways off [22]. To ensure the security of user data in cloud computing, a number of encryption methods have been proposed, including Diffie-Hellman [23] and a hybrid system that combines RSA, 3DES, and random number generator [24].

- *Encrypted Search and Database*

Since the homomorphic encryption method is ineffective when used in cloud environments, the restricted homomorphic encryption algorithm was developed, leading to the widespread use of encrypted search [22]. The transposition, substitution, folding, and shifting (TSFS) algorithm is one of the numerous ideas of this kind. It is a simple method for encrypting databases [25]. (2) To protect sensitive data in an untrusted cloud environment, an in-memory database encryption solution is used. (3) Asymmetric encryption for cloud-based databases [26]. (4) A multikeyword ranked search strategy that protects privacy via encrypted cloud data [27].

- *Data Concealment*

In the cloud, data secrecy can be guaranteed through data hiding. A concealing idea was put up by Delettre et al. [28] for database security. The visual fake data is combined with genuine data to distort the volume of the real data, and authorized users can utilize watermarking to distinguish between the fake and real data. Data hiding aims to protect sensitive information from nefarious users.

- *Distributive Storage*

We can store data in many clouds or cloud databases to guarantee data integrity; this has emerged as a viable method in the cloud environment [22]. A method for achieving that was put up by Ram et al. [29] who introduced the concept of security as a service for cloud data security. To achieve utmost security, the technique relied on segmenting the user's data into smaller bits. The idea of data distribution overcloud is formed by encrypting these data pieces and storing them in different databases.

B. Data Integrity

In cloud computing, data integrity refers to the idea that data shouldn't be lost or altered by unauthorized access. This is the foundation for cloud computing services, particularly DBaaS. Authorization is a critical component that ensures that only authorized entities may interact with data, which ultimately leads to higher trust in data integrity. This is because cloud environments have a huge number of entities and access points. Furthermore, monitoring systems can offer excellent visibility into identifying potential data alterers and how they may have impacted the data's integrity. Lastly, as cloud computing environments typically include data processing services, methods like digital signatures and RAID-like procedures can be used to obtain data integrity [22].

C. Data Availability

One of the most important security factors that businesses must take into account when offering cloud database services is the requirement that databases in the cloud be highly available and dependable [10, 30]. One known assault that compromises data availability is the Dos attack. Cloud data storage needs to be redundantly stored using distributed storage techniques and backups in order to do that. Because traditional relational databases struggle with high performance, large storage, and scalability, NoSQL databases were created and work better in cloud computing environments. Additionally, since the backup disk database can restore data quickly, distributed database proxies can offer high availability [25]. Lastly, before switching to a cloud database, consideration should be given to the availability level, data backup choices, and disaster recovery strategies.

D. Data Isolation

In cloud computing, there are various types of data. For example, data in deployed applications can comprise user account information and contents generated or utilized by the application. Techniques for access control and data encryption are used to protect data from unwanted access. Since most access controls are identity-based, user identity authentication is crucial, and there are problems with it in cloud computing. Different database arrangements are available in the multi-tenant model. These arrangements pool resources in different ways and provide varying levels of resource efficiency and isolation. Data encryption, for example, can be used with setups that use distinct databases instead of common databases.

E. Data Privacy

The loss of privacy is a major deterrent to cloud database deployment since it undermines user confidence in the system.
To allay privacy worries, clients can use data encryption for any stored data within the DBaaS. This raises the efficiency difficulty [31] and begs the question of how the DBaaS can run queries over the encrypted data.
Thus, as was already indicated, a number of methods were put out to address the encrypted data query issue. For instance, [7] suggested a design architecture to address data privacy issues by integrating CryptDB into the relational

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 November 2023*

cloud (transactional DBaaS). An MIT researcher presented CryptDB, a solution that provides verifiable and useful data secrecy for SQL database-based applications.

F. Data Sanitization

In order to prevent any unwanted disclosure of data, the sanitization procedure entails the efficient deletion of data from storage media by overwriting, degaussing, or destroying the medium itself. Multiple customers' data are physically co-located together in a public cloud environment, which complicates the sanitization procedure. Further complicating matters are the data backups that are performed to provide high redundancy[6]. Irreversible resources, non-wiped hard drives used by several tenants, and inadequate application of destruction policies all contribute to problems with data sanitization[27].

V. CLOUD DATABASE SECURITY ISSUES

This section examines the security issues that the database faces when operating in a cloud environment.

A. Insecure Application Programming Interfaces (API)

Cloud computing providers provide a set of software interfaces for APIs, which enable providers to carry out provisioning, management, orchestration, and monitoring. These interfaces enable customers to manage and engage with cloud services. The security of these APIs is what determines the availability and security of cloud services. Thus, in addition to encryption and activity tracking, APIs need to include authentication and access control. Furthermore, these interfaces need to be resistant to attempts to revoke regulations, whether intentional or unintentional [32].

B. Authentication and Access Control (AAC) Issues

Broken authentication and session control threats, which arise from improper configuration of account management functions, are the main security concerns in AAC. For instance, an attacker may exploit exposed user session IDs that appear in the URL as a result of password, key, and session token compromises.

C. Cloud Database Misconfigurations

Some cloud service providers do a poor job of providing their clients with auditing and monitoring options. Due to problems with cloud misconfiguration, this could result in failures and breaches. Because the cloud database environment is dynamic, reliance on standard configuration is no longer useful. Consequently, regardless of the location of the database, cloud providers need to provide an auditing method or tool that generates complete visibility into database activity [35].

D. Multi-Tenancy Vulnerability

The data isolation problem is one of the main security issues in a multi-tenant database system. Since several tenants (users/customers) are accessing the same database through a multi-tenant database, cloud providers ought to offer segregated database access for each tenant. Make sure that data protection and user privacy are positively impacted by data isolation. However, failing to provide data isolation could result in data exposure and security lapses [36].

E. Data Loss or Leakage

The quantity and interactions between risks and problems that are either specific to the cloud or more risky because of its operational or architectural features increase the potential of data compromise in the cloud environment. The deletion or modification of records without a suitable backup might result in data loss. When documents from larger records are not properly linked and are destroyed or altered, data cannot be recovered. Losing the encoding key might also cause actual devastation[11].

F. Account, Service and Traffic Hijacking

This danger encompasses a variety of threats, including software exploitation, fraud, and phishing. Once the attacker has access to the credentials for the account, they can use them to change data, spy on transactions and activities, provide misleading information, and send users to malicious websites. Restricting account sharing between a client and the service providers is crucial to reducing these attacks. Additionally, it's critical to use proactive monitoring tools and two-way authentication procedures to identify suspect or unauthorized activity [15].

G. Malicious Injection Attack

SQL servers running susceptible database applications are the target of this attack. Attackers use malicious script injections to circumvent authentication and obtain unauthorized access to backend databases by taking advantage of vulnerabilities in web servers. If successful, attackers can use SQL script injection to change database contents, obtain private information, run system instructions remotely, or utilize the web server for later purposes. A botnet can also deliver a SQL injection attack; one example of this is the Asprox botnet, which was able to control a thousand bots that were outfitted with a SQL injection kit and were ready to launch a SQL injection assault. Six million URLs belonging to various 153,000 websites were targeted by this botnet [37].

H. Insider Threats

Every business organization is familiar with the threat posed by a malicious insider. The cloud environment makes this security threat more apparent. due to the integration of service providers and clients into a single management sector, as well as the lack of openness in the process and procedure offering,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 November 2023*

which will ultimately lead to a security flaw. By performing an evaluation of supply chain management and making sure that stringent regulations are followed, this problem can be resolved [32].

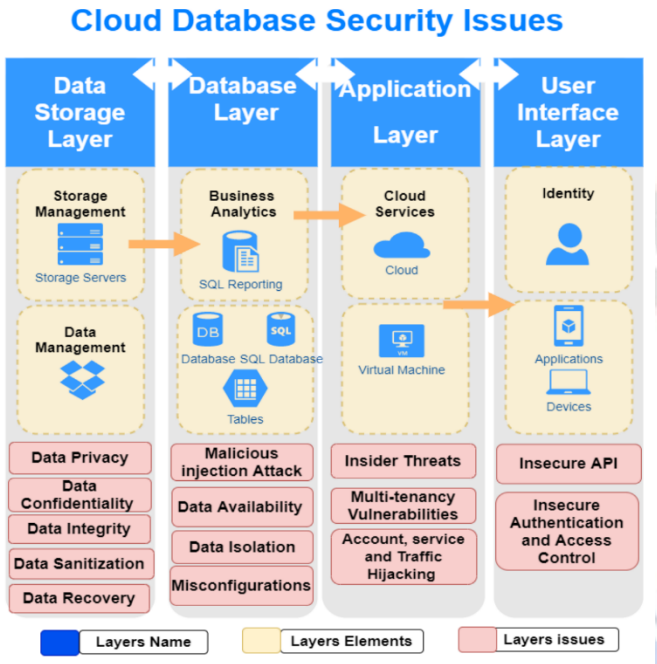

Figure 2. A Conceptual Model for Understanding the Cloud Database Security Issues

VI. CONCLUSIONS

Some open issues can be introduced for additional future research and investigation based on the analysis and discussion of cloud database security challenges. Effective Encryption: Strong encryption methods that are also suitable for cloud systems are desperately needed. The suggested algorithms should decrease delay by not placing an extra strain on cloud activities. The confidentiality and integrity can be protected with the right encryption techniques.

Improved Data Privacy Plans: For all cloud services, data privacy is a top priority. There has to be more privacy-preserving schemes. These programs ought to protect client data and lessen any infractions by service providers. Enhanced Trust Programs: The majority of cloud users worry about how much faith they can place in cloud service providers. As a result, it is crucial to raise the degree of confidence by appropriately enlisting the assistance of a third party.

Schemes for Application-Level Protection: As seen in Fig. 2, the data security may be jeopardized by the database management application's vulnerability, particularly if authorized insiders take use of it. In addition, safeguarding against the exploitation of applications and services is a critical matter that requires attention. For cloud database management systems, application-based protection mechanisms are therefore necessary.

Cloud computing has been widely adopted during the past 10 years, giving rise to the idea of Database as a Service (DBaaS), which has piqued the interest of both industry and research community. In addition, a lot of businesses have begun utilizing cloud computing and gaining access to their data via cloud databases. However, security has been found to be the biggest threat to cloud databases. This includes concerns with data protection and can result in major security problems including multi-tenancy vulnerabilities and insecure APIs. Nonetheless, cryptography and safe storage options are necessary for cloud database security. Furthermore, even if there are still a lot of unresolved problems, combining encryption with SQL operations within the cloud database is a viable strategy. We addressed the modern security concerns and obstacles in this work that can prevent cloud databases from being widely used. In order to help with better cloud database provider selection, we have also proposed a conceptual model that summarizes and clarifies these challenges and their impact on cloud databases. Lastly, we highlight how businesses evaluate cloud database providers according to their security requirements.

It is evident that scholars are interested in making a contribution to this topic by studying the security of cloud databases. Future directions can include data sanitization (as yet unresolved issue), safe access control, privacy (anonymize and encrypt data), and encryption solutions (simplified encryption approaches).

REFERENCES

[1] Armbrust, M., et al., A view of cloud computing. Communications of the ACM, 2010. 53(4): p. 50-58.
[2] Kuyoro, S., F. Ibikunle, and O. Awodele, Cloud computing security issues and challenges. International Journal of Computer Networks (IJCN), 2011. 3(5): p. 247-255.
[3] Weis, J. and J. Alves-Foss, Securing database as a service: Issues and compromises. IEEE Security & Privacy, 2011. 9(6): p. 49-55.
[4] Al Shehri, W., Cloud database database as a service. International Journal of Database Management Systems, 2013. 5(2): p. 1.
[5] Khan, S., et al., Bivariate, Cluster and Suitability Analysis of NoSQL Solutions for Different Application Areas. arXiv preprint arXiv:1911.11181, 2019.
[6] Sakhi, I., Database security in the cloud. 2012.
[7] Curino, C., et al., Relational cloud: A database-as-a-service for the cloud. 2011.
[8] Deka, G.C., A survey of cloud database systems. It Professional, 2013. 16(2): p. 50-57.
[9] Mongo, D., Nosql databases explained.
[10] Alam, M. and K.A. Shakil, Cloud database management system architecture. UACEE International Journal of Computer Science and its Applications, 2013. 3(1): p. 27-31.
[11] Satish, Karuturi S R V, and M Swamy Das. "Quantum Leap in Cluster Efficiency by Analyzing Cost-Benefits in Cloud Computing." In Computer Science and Engineering by Auroras Scientific Technological & Research Academy Hyderabad, vol. 17, no. 2, pp. 58-71. Accessed 2018. https://www.ijsr.in/article-description.php?id=ZU9rWnA5d3R1Q1dzK2tLSTNTbDRZZz09.
[12] CSA, CSA Releases New Research - Top Threats to Cloud Computing: Egregious Eleven. 2019, Cloud Security Allowance (CSA).

[13] Sawant, N., V. Pottigar, and N. Mane. A survey on auditing techniques used for preserving privacy of data stored on cloud. in 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT). 2016. IEEE.
[14] Gong, S. and X.X. Huang. Study on database encryption-based protection mechanism under cloud computing environment. in 2016 2nd IEEE International Conference on Computer and Communications (ICCC). 2016. IEEE.
[15] Han, J., et al. Survey on NoSQL database. in 2011 6th international conference on pervasive computing and applications. 2011. IEEE.
[16] Yaseen, Q. and B. Panda. Tackling insider threat in cloud relational databases. in 2012 IEEE Fifth International Conference on Utility and Cloud Computing. 2012. IEEE.
[17] Ramachandra, G., M. Iftikhar, and F.A. Khan, A comprehensive survey on security in cloud computing. Procedia Computer Science, 2017. 110: p. 465-472.
[18] Satish, Karuturi S R V, and M Swamy Das. "Review of Cloud Computing and Data Security." IJAEMA (The International Journal of Analytical and Experimental Modal Analysis) 10, no. 3 (2018): 1-8.
[19] Sen, J., Security and privacy issues in cloud computing, in Cloud Technology: Concepts, Methodologies, Tools, and Applications. 2015, IGI Global. p. 1585-1630.
[20] Alam, B., et al., 5-layered architecture of cloud database management system. AASRI Procedia, 2013. 5: p. 194-199.
[21] Hussain, S.A., et al., Multilevel classification of security concerns in cloud computing. Applied Computing and Informatics, 2017. 13(1): p. 57-65.
[22] Sun, Y., et al., Data security and privacy in cloud computing. International Journal of Distributed Sensor Networks, 2014. 10(7): p. 190903.
[23] Boneh, D. The decision diffie-hellman problem. in International Algorithmic Number Theory Symposium. 1998. Springer.
[24] Kaur, A. and M. Bhardwaj, Hybrid encryption for cloud database security. Journal of Engineering Science Technology, 2012. 2: p. 737-741.
[25] Han, J., M. Song, and J. Song. A novel solution of distributed memory nosql database for cloud computing. in 2011 10th IEEE/ACIS International Conference on Computer and Information Science. 2011. IEEE.
[26] Sedayao, J. and I.I. Enterprise Architect, Enhancing cloud security using data anonymization. White Paper, Intel Coporation, 2012.
[27] Satish, Karuturi S R V, and M Swamy Das. "Multi-Tier Authentication Scheme to Enhance Security in Cloud Computing." IJRAR (International Journal of Research and Analytical Reviews) 6, no. 2 (2019): 1-8.
[28] Delettre, C., K. Boudaoud, and M. Riveill. Cloud computing, security and data concealment. in 2011 IEEE Symposium on Computers and Communications (ISCC). 2011. IEEE.
[29] Ram, C.P. and G. Sreenivaasan. Security as a service (sass): Securing user data by coprocessor and distributing the data. in Trendz in Information Sciences & Computing (TISC2010). 2010. IEEE.
[30] Bollavarapu, S. and K. Mistry, Secure Database as a Service-a Review. International Journal of Advanced Research in Computer and Communication Engineering Vol, 2015. 4: p. 425-429.
[31] Izang, A., et al., Security and ethical issues to cloud database. Journal of Computer Science and Its Application, 2017. 24(2): p. 65-75.
[32] Malhotra, S., et al., Cloud Database Management System security challenges and solutions: an analysis. CSI transactions on ICT, 2016. 4(2-4): p. 199-207.
[33] Kumar, P.R., P.H. Raj, and P. Jelciana, Exploring data security issues and solutions in cloud computing. Procedia Computer Science, 2018. 125: p. 691-697